RESEARCH and INNOVATION

AT EMBRY-RIDDLE

REDAC SAS
Aviation Cybersecurity & Research Needs

March 2, 2022

Dan Diessner

Associate Director – Center of Aerospace Resilience; Embry Riddle Aeronautical University

TLP WHITE

Aviation Cyber Safety Considerations

Agenda: (target 20 minutes of charts then leave time for discussion)

- DHS Traffic Light (TLP) Protocol
- Cyber Framework Research Considerations
- Some personal history – just one person's perspective.
- ARAC ASISP Working Group - Final Report August 22, 2016
- Cyber Safety Commercial Aviation Team – 2020 Industry / Government Workshops
- Aerospace Industry Association: Civil Aviation Cybersecurity Subcommittee
- 2021 ERAU Symposium on Aero Cyber Resilience – CISO Panel Thoughts
- Summary for FAA Future Research: Possible Cyber Safety Related Topics

Dan Diessner

DHS Traffic Light (TLP) Protocol

As a critical infrastructure, the Aviation Industry uses the DHS TLP protocol to appropriately mark security data based on its sensitivity and sharing criteria.

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Source: Table provided by NPPD U.S. Computer Emergency Readiness Team (US-CERT)

Dan Diessner

Cyber Framework Research Considerations

- All business considerations
- Consider Research Context
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

Figure 6: NIST Cybersecurity Framework Core components.
Source: National Institute of Standards and Technology (2018)

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

What should we be doing & researching to maintain the cyber-resilience & cyber-safety of the aviation ecosystem?

I have been wandering the path of this growing challenge for many years:

- 777 Network Systems: 1989-1996 – The initial recognition of cybersecurity risks
  - 1st aircraft COTS based networking technologies (Ethernet & FDDI); SW Data Load; Security measure soon after
- Cabin & Network Systems R&D: 1997-2002 (early development)
  - ARINC 664 development days, initial proliferation of COTS networking technologies primarily in Cabin Systems… et al.
- USAF VIP/SAM Fleet Mx/Mods/Upgrades: 2004-1013 (full cyber appreciation)
- BCA Chief Engineering Airplane Systems Product Development & New Technologies: 2013-2015
- BCA Product Cybersecurity: 2015-2021 – Retired after 34+ years @ Boeing
  - ARAC ASISP, A-ISAC, ACI, ICAO TFSG / SSGC, Stood up AIA Civil Cybersecurity SC, Cyber Safety Commercial Aviation Team, etc.
  - Independent Cyber Researchers: various levels of legitimacy, e.g. Black Hat DEF CON 2018/2019/2020 on Satellite systems & Aircraft SW
- ERAU Center for Aviation Resilience (~1+ year)
  - Annual Aero Cyber Symposium – now I get to pick the brains of a lot more of really smart people from across aviation

ARAC ASISP Working Group
Final Report August 22, 2016

Recommendation Research R1: The ASISP recommends that the FAA consider the following topics as part of future agency research to address cybersecurity (Section 5.3):

- ✓ The FAA should undertake research to determine how threat and vulnerability sharing can be most effectively done for ASISP including in coordination with international partners and regulators.
- ✓ The FAA should fund the development of tools that can facilitate event log analysis.
- ? Study means of detecting and preventing vulnerabilities from PED's connectivity to Avionic Interface Devices.
- ✓ Study means of detecting vulnerabilities in receiving transponder and ADS-B Data in aircraft.

ARAC: Aviation Rulemaking Advisory Committee
ASISP: Aircraft System Information Security / Protection (ASISP)

Dan Diessner

Cyber Safety Commercial Aviation Team 2020 Industry / Government Workshops

Founded March 2019, the Cyber Safety Commercial Aviation Team (CSCAT) was established by US Aviation Industry Cyber Leaders in cooperation with US Government Cyber Leaders (FAA, DHS, DoD). Like CAST, it was established to evaluate known safety risks, but those that are Cyber Safety in nature. The CSCAT is positioned to look into known cyber safety risk scenarios that may exist, execute a risk analysis study and provide recommendations as appropriate.

2020 the Cyber Safety Commercial Aviation Team (CSCAT) led a series of workshops of ~50+ Industry and Government aviation cyber experts to identify areas of potential cyber evaluation. The group agreed on the top 3 of greatest potential for cyber safety impacts in civil aviation if compromised.

1. Navigation Systems
2. Supply Chain Cybersecurity
3. Avionics Databus / Network Interfaces

CAST: Commercial Aviation Safety Team

Dan Diessner

Aerospace Industry Association
Civil Aviation Cybersecurity Subcommittee

Civil Aviation Cybersecurity (https://www.aia-aerospace.org/issue/cyber-security/ **)**

- Maintaining that safety performance and protecting the operations and reputation of the civil aviation industry is a shared responsibility of the global aviation community. This is accomplished by means of commonly held vision, strategies, goals, standards, implementation models, and international policies.
- The same approach must be adopted for commercial aviation product cybersecurity to provide continued cyber-safety and cyber-resiliency as the aviation world becomes more connected.
- Read the recommendations on how to address evolving threats from AIA's Civil Aviation Cybersecurity Subcommittee.
- Read the final report on Software Cyber Recommendations.
- Read our recent report on Cybersecurity Testing Recommendations.
- Read AIA's recommendations report on Civil Aviation Software Cybersecurity.
- Read our 2021 Civil Aviation Cybersecurity Annual Report.

Dan Diessner

2021 ERAU Symposium on Aero Cyber Resilience – Executive Panel Thoughts

Top Areas for Research:

1. PNT (i.e. GPS…)
2. Aviation Maintenance
3. Remote Attestation / Secure Boot
4. Coms Digital Trust - Integrity / Compromise
5. Aircraft Operational Data Security

[Supply Chain theme throughout.]

Panel included top cyber leaders representing US aviation OEM, Airline, FAA, DoD and also ICAO.

Panel Overview

Each Panel Member will now be given a few minutes to address the following questions regarding Aero Cybersecurity & our aviation and aerospace community research needs:

1. What would you like to share about yourself and your experiences?
2. What keeps you awake at night?
3. What should we being doing about it, that we can do better together?

[Note: All members approved for me to share this with the REDAC SAS as the panel leader.]

Dan Diessner

Summary for FAA Future Research Possible Cyber Safety Related Topics

1. Harnessing and analyzing data (What and How?) A/C Security Log Data, MOC Requirements & Tools to support emerging regulatory requirements (e.g. AI).
2. Secure Digital Coms – ACARS, IPS, etc.. (some possibly addressed elsewhere, e.g. ongoing IPS efforts.)
3. Remote Attestation / Secure Boot.
4. Supply chain cybersecurity.
5. Cloud interface with Aircraft Operations.
6. Cybersecurity testing impact of aircraft avionics (Can research be done to show potential risks of PEN testing aircraft? Do we need better controls?).
7. Airborne Software Security? Maybe we know what we need for now. Also see AIA SW Security Report.

Included in 3/2022 Consideration List

Additional Possible Future Consideration

Conclusion: Need a well informed and balanced approach to maintain aviation cyber safety and cyber resilience as aviation becomes more hyper connected.

Caution: It is easy to buy into connectivity changes for good performance reasons and not adequately consider the cyber risks introduced.

Dan Diessner

Discussion – Comments – Questions